AMENDMENTS TO THE CLAIMS

Claim 1 (Previously Presented) An encryption communication system for secret message communication, the encryption communication system comprising an encryption transmission apparatus and an encryption reception apparatus,

wherein the encryption transmission apparatus includes:

a storage unit that stores one message;

an encryption unit operable to perform an encryption computation on the one message a plural number of times to generate a plurality of encrypted messages from the one message, a number of encrypted messages generated from the one message by the encryption unit being equal to the number of times the encryption unit performs the encryption computation on the one message;

a computation unit operable to perform a one-way operation on the one message to generate only one comparison computation value from the one message; and

a transmission unit operable to transmit, to the encryption reception apparatus, the plurality of the encrypted messages and the one comparison computation value, and

wherein the encryption reception apparatus includes:

a reception unit operable to receive, from the encryption transmission apparatus, the plurality of the encrypted messages and the one comparison computation value;

a decryption unit operable to perform a decryption computation corresponding to the encryption computation, the decryption computation being performed on each of the encrypted messages to generate a plurality of decrypted messages, and a number of decrypted messages generated by the decryption unit being equal to the number of encrypted messages

generated from the one message by the encryption unit;

a computation unit operable to perform the one-way operation on each of the decrypted messages to generate a plurality of decryption computation values, a number of decryption values generated by the computation unit being equal to the number of the decrypted messages generated by the decryption unit; and

a judging unit operable to compare each of the decryption computation values with the one received comparison computation value,

wherein (i) when at least one of the decryption computation values matches the one received comparison computation value, the judging unit outputs a decrypted message as a correct decrypted message, and (ii) when none of the decryption computation values matches the one received comparison computation value, the judging unit determines that there is a decryption error.

Claim 2 (Previously Presented) The encryption communication system of Claim 1,

wherein the encryption computation used by the encryption unit conforms to NTRU cryptosystem, and

wherein the decryption computation used by the decryption unit conforms to the NTRU cryptosystem.

Claim 3 (Previously Presented) An encryption transmission apparatus for secret message communication with an encryption reception apparatus, the encryption transmission apparatus comprising:

a storage unit that stores one message;

an encryption unit operable to perform an encryption computation on the one message a plural number of times to generate a plurality of encrypted messages from the one message, a number of encrypted messages generated from the one message by the encryption unit being equal to the number of times the encryption unit performs the encryption computation on the one message;

a computation unit operable to perform a one-way operation on the one message to generate only one comparison computation value from the one message; and

a transmission unit operable to transmit, to the encryption reception apparatus, the plurality of the encrypted messages and the one comparison computation value.

Claim 4 (Previously Presented) The encryption transmission apparatus of Claim 3, wherein the encryption unit comprises:

an encryption computation subunit operable to perform an invertible data conversion on the one message to generate a converted message, and perform an encryption algorithm on the converted message to generate one encrypted message; and

a repetition control subunit operable to control the encryption computation subunit to repeat the generation of the converted message and the generation of the one encrypted message, the generation of the converted message and the generation of the one encrypted message being repeated the plural number of times the encryption unit performs the encryption computation on the one message to generate the plurality of encrypted messages.

Claim 5 (Previously Presented) The encryption transmission apparatus of Claim 4, wherein the encryption computation subunit generates a random number of a fixed length, and generates the converted message by adding the random number to the one message.

Claim 6 (Previously Presented) The encryption transmission apparatus of Claim 5, wherein the encryption algorithm used by the encryption computation subunit on the converted message conforms to NTRU cryptosystem.

Claim 7 (Previously Presented) An encryption reception apparatus for secret message communication with an encryption transmission apparatus, the encryption transmission apparatus storing one message, performing an encryption computation on the one message a plural number of times to generate a plurality of encrypted messages from the one message, a number of encrypted messages generated from the one message by the encryption transmission apparatus being equal to the number of times the encryption transmission apparatus performs the encryption computation on the one message, performing a one-way operation on the one message to generate only one comparison computation value from the one message, and transmitting, to the encryption reception apparatus, the plurality of encrypted messages and the one comparison computation value, the encryption reception apparatus comprising:

a reception unit operable to receive, from the encryption transmission apparatus, the plurality of the encrypted messages and the one comparison computation value;

a decryption unit operable to perform a decryption computation corresponding to the encryption computation, the decryption computation being performed on each of the encrypted

messages to generate a plurality of decrypted messages, and a number of decrypted messages generated by the decryption unit being equal to the number of encrypted messages generated from the one message by the encryption transmission apparatus;

a computation unit operable to perform the one-way operation on each of the decrypted messages to generate a plurality of decryption computation values, a number of decryption computation values generated by the computation unit being equal to the number of the decrypted messages generated by the decryption unit; and

a judging unit operable to compare each of the decryption computation values with the one received comparison computation value,

wherein (i) when at least one of the decryption computation values matches the one received comparison computation value, the judging unit outputs a decrypted message as a correct decrypted message, and (ii) when none of the decryption computation values matches the one received comparison computation value, the judging unit determines that there is a decryption error.

Claim 8 (Previously Presented) The encryption reception apparatus of Claim 7,

wherein the encryption transmission apparatus performs an invertible data conversion on the one message to generate a converted message, performs an encryption algorithm on the converted message to generate one encrypted message, and repeats the generation of the converted message and the generation of the one encrypted message, the generation of the converted one message and the generation of the one encrypted message being repeated the plural number of times the encryption unit performs the encryption computation on the one

message to generate the plurality of encrypted messages, and

wherein the decryption unit comprises:

a decryption computation subunit operable to perform a decryption algorithm corresponding to the encryption algorithm, on one of the plurality of the encrypted messages to generate one decrypted text, and perform an inverse conversion of the invertible data conversion on the one decrypted text to generate one decrypted message; and

a repetition control subunit operable to control the decryption computation subunit to repeat the generation of the one decrypted content and the generation of the one decrypted message, the generation of the one decrypted content and the generation of the one decrypted message being repeated the plural number of times the decryption unit performs the decryption computation to generate the plurality of the decrypted messages being equal in number to the number of encrypted messages generated from the one message by the encryption unit.

Claim 9 (Previously Presented) The encryption reception apparatus of Claim 8,

wherein the encryption transmission apparatus generates a random number of a fixed length, and generates the converted message by adding the random number to the one message, and

wherein the decryption computation subunit generates the one decrypted message by removing the random number of the fixed length from the one decrypted text.

Claim 10 (Previously Presented) The encryption reception apparatus of Claim 9,

wherein the encryption algorithm used by the encryption transmission apparatus conforms to NTRU cryptosystem, and

wherein the decryption algorithm used by the decryption computation subunit conforms to the NTRU cryptosystem.

Claim 11 (Previously Presented) An encryption transmission method used in an encryption transmission apparatus, the encryption transmission apparatus storing one message and transmitting the one message in secrecy to an encryption reception apparatus, the encryption transmission method comprising:

performing an encryption computation on the one message a plural number of times to generate a plurality of encrypted messages from the one message, a number of encrypted messages generated from the one message by the performing of the encryption computation being equal to the number of times the performing of the encryption computation performs the encryption computation on the one message;

performing a one-way operation on the one message to generate only one comparison computation value from the one message; and

transmitting, to the encryption reception apparatus, the plurality of the encrypted messages and the one comparison computation value.

Claim 12 (Previously Presented) A computer-readable recording medium having an encryption transmission program recorded thereon, the encryption transmission program being used in an encryption transmission apparatus, the encryption transmission apparatus storing one

message and transmitting the message in secrecy to an encryption reception apparatus, the encryption transmission program causing the encryption transmission apparatus to execute a method comprising:

performing an encryption computation on the one message a plural number of times to generate a plurality of encrypted messages from the one message, a number of encrypted messages generated from the one message by the performing of the encryption computation being equal to the number of times the performing of the encryption performs the encryption computation on the one message;

performing a one-way operation on the one message to generate only one comparison computation value from the one message; and

transmitting, to the encryption reception apparatus, the plurality of the encrypted messages and the one comparison computation value.

Claim 13 (Cancelled)

Claim 14 (Previously Presented) An encryption reception method used in an encryption reception apparatus, the encryption reception apparatus receiving a message from an encryption transmission apparatus in secrecy, the encryption transmission apparatus storing one message, performing an encryption computation on the one message a plural number of times to generate a plurality of encrypted messages from the one message, a number of encrypted messages generated from the one message by the encryption transmission apparatus being equal to the number of times the encryption transmission apparatus performs the encryption computation on

the one message, performing a one-way operation on the one message to generate only one comparison computation value from the one message, and transmitting, to the encryption reception apparatus, the plurality of encrypted messages and the one comparison computation value, the encryption reception method comprising:

receiving, from the encryption transmission apparatus, the plurality of the encrypted messages and the one comparison computation value;

performing a decryption computation corresponding to the encryption computation, the decryption computation being performed on each of the encrypted messages to generate a plurality of decrypted messages, and a number of decrypted messages generated by the performing of the decryption computation being equal to the number of encrypted messages generated from the one message by the encryption transmission apparatus;

performing the one-way operation on each of the decrypted messages to generate a plurality of decryption computation values, a number of decryption computation values generated by the performing of the one-way operation being equal to the number of the decrypted messages generated by the performing of the decryption computation;

comparing each of the decryption computation values with the one received comparison computation value;

outputting a decrypted message that corresponds to a decryption computation value that matches the one received comparison computation value, based on the comparing, as a correct decrypted message when at least one of the plurality of the decryption computation values matches the one received comparison computation value; and

determining that there is a decryption error when, as a result of the comparing, none of

the decryption computation values matches the one received comparison computation value.

Claim 15 (Previously Presented) A computer-readable recording medium having an encryption reception program recorded thereon, the encryption reception program being used in an encryption reception apparatus, the encryption reception apparatus receiving a message from an encryption transmission apparatus in secrecy, the encryption transmission apparatus storing one message, performing an encryption computation on the one message a plural number of times to generate a plurality of encrypted messages from the one message, a number of encrypted messages generated from the one message by the encryption transmission apparatus being equal to the number of times the encryption transmission apparatus performs the encryption computation on the one message, performing a one-way operation on the one message to generate only one comparison computation value from the one message, and transmitting, to the encryption reception apparatus, the plurality of encrypted messages and the one comparison computation value, the encryption reception program comprising:

receiving, from the encryption transmission apparatus, the plurality of the encrypted messages and the one comparison computation value;

performing a decryption computation corresponding to the encryption computation, the decryption computation being performed on each of the encrypted messages to generate a plurality of decrypted messages, and a number of decrypted messages generated by the performing of the decryption computation being equal to the number of encrypted messages generated from the one message by the encryption transmission apparatus;

performing the one-way operation on each of the decrypted messages to generate a

plurality of decryption computation values, a number of decrypted computation values generated by the performing of the one-way operation being equal to the number of the decrypted messages generated by the performing of the decryption computation;

comparing each of the decryption computation values with the one received comparison computation value;

outputting a decrypted message that corresponds to a decryption computation value that matches the one received comparison computation value, based on the comparing, as a correct decrypted message when at least one of the plurality of the decryption computation values matches the one received comparison computation value; and

determining that there is a decryption error when, as a result of the comparing, none of the decryption computation values matches the one received comparison computation value.

Claim 16 (Cancelled)

Claim 17 (New) The encryption communication system of Claim 1,

wherein the encryption unit performs a predetermined computation on the one message a plural number of times to generate a plurality of computation results, and performs the encryption computation on each computation result of the generated plurality of computation results to generate the plurality of encrypted messages from the one message, and

wherein the decryption unit performs the decryption computation on each encrypted message of the generated plurality of encrypted messages to generate a plurality of decryption results, and performs an inverse computation of the predetermined computation on each

decryption result of the generated plurality of decryption results the plural number of times to generate the plurality of decrypted messages.

Claim 18 (New) The encryption transmission apparatus of Claim 3,

wherein the encryption unit performs a predetermined computation on the one message a plural number of times to generate a plurality of computation results, and performs the encryption computation on each computation result of the generated plurality of computation results to generate the plurality of encrypted messages from the one message.

Claim 19 (New) The encryption reception apparatus of Claim 7,

wherein the encryption transmission apparatus performs a predetermined computation on the one message a plural number of times to generate a plurality of computation results, and performs the encryption computation on each computation result of the generated plurality of computation results to generate the plurality of encrypted messages from the one message, and

wherein the decryption unit performs the decryption computation on each encrypted message of the generated plurality of encrypted messages to generate a plurality of decryption results, and performs an inverse computation of the predetermined computation on each decryption result of the generated plurality of decryption results the plural number of times to generate the plurality of decrypted messages.